引 用 文 献 5

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 99/05816

(43) International Publication Date: 4 February 1999 (04.02.99)

(21) International Application Number: PCT/IL98/00342

(22) International Filing Date: 23 July 1998 (23.07.98)

(30) Priority Data:
121389 24 July 1997 (24.07.97) IL

(71) Applicant *(for all designated States except US)*: GRAPHITECH LTD. [IL/IL]; Herzl Street 25, 51364 Bnei-Braq (IL).

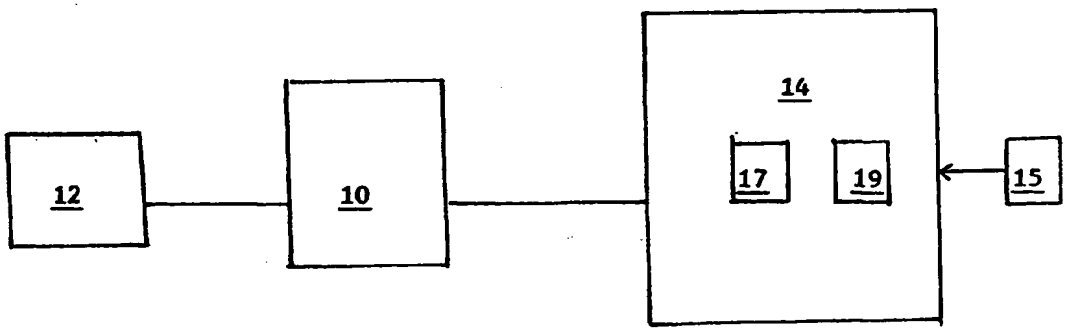
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BAR NATAN, Nir [IL/IL]; Apartment 5, Harei Yehudah Street 50, 55900 Ganei Tikvah (IL). BASSAN, Jonathan [IL/IL]; Hanoter Street 2, 47210 Ramat Hasharon (IL). GROZOVIK, Oren [IL/IL]; Lamdan Street 12, 69414 Tel Aviv (IL). WAISEL, Shai [IL/IL]; Hazait Street 6, 49214 Petach Tikvah (IL).

(74) Agent: SELIGSOHN & GABRIELI; P.O. Box 1426, 61013 Tel Aviv (IL).

(81) Designated States: JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING SIGNATURES



(57) Abstract

A system and method for authenticating a signature, the system including a digitizer (10) and associated electronic pen (12), a dynamic identification unit (14) for receiving data from the digitizer (10) produced during the signature by the electronic pen (12) on the digitizer (10), calculating signature parameters and permitted variations from the data, and generating a reference record (15) therefrom, a comparator (17) for comparing the received parameters produced during signature with the reference record (15), and apparatus for providing an accept or reject response in accordance with the output of the comparator (17).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM AND METHOD FOR AUTHENTICATING SIGNATURES

FIELD OF THE INVENTION

The present invention relates to a system and method for authenticating signatures in general and, in particular, to a system and method for authenticating signatures transmitted over digital communication lines.

BACKGROUND OF THE INVENTION

In the field of computer graphics, it is known to use a digitizer to convert graphical data into electronic data for a computer. A user draws with an electronic pen on the digitizer tablet, and the digitizer converts the graphical data to electric signals. Such digitizers are used today for inputting data to computers, similar to a mouse.

There are many occasions in which it is necessary to authenticate the signature of a person signing a document in order to ensure that the signatory is indeed the person whose name is being signed. One particular application is the field of credit cards, wherein sums of money change hands in reliance on the signature of the card holder. In the event that a card is stolen, a person who can forge the cardholder's signature can charge items against the cardholder's bank account. Similarly, when purchases are made over the telephone, the number and expiration date of the card are read to the vendor, but there is no way to verify whether the caller is an authorized user of the card.

This problem has reached new heights with the advent of the Internet, where sales are transacted by means of transmitting the number and expiration date of the credit card only, without any means of verifying the origin of the purchase. Since these communication lines are open, it is easy for a hacker to determine the number and expiration date of someone else's credit card which were transmitted over his modem, and to use that credit card for unauthorized purchases.

Authentication of signatures by means of a graphical image (or bitmap) is not a solution because a photocopy of the signature looks authentic and cannot be detected.

Accordingly, there is a long felt need for and it would be very desirable to have a method of authenticating the signature of a person, particularly a person using a credit card, both in a conventional sales transaction in a store, and over transmission lines, such as the Internet.

SUMMARY OF THE INVENTION

According to the present invention, there is provided a system for authenticating a signature including a digitizer, an electronic pen, a dynamic identification unit for measuring vectors produced during signature by the electronic pen on the digitizer, and a comparator for comparing the vectors produced during signature with a reference signature.

According to a preferred embodiment, the system also includes an encryptor for encrypting a signature record and a decoder for decoding the encrypted signature record.

According to another preferred embodiment, the reference signature record is stored on an IC (integrated chip) card.

In accordance with the present invention, there is also provided a method of authenticating a signature including the steps of

providing a reference signature record,

signing with an electronic pen on a digitizer tablet,

calculating parameters from data produced during signing on the digitizer tablet;

comparing the parameters produced during signature with a reference signature record; and

providing an accept or reject response in accordance with results of the comparison.

According to a preferred embodiment, the method also includes the steps of encrypting the calculated parameters

with a encryption key, and decrypting the encrypted data before comparing the parameters.

Further according to a preferred embodiment, the method includes the step of transmitting the calculated parameters over a transmission line to a remote location before the step of comparing.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be further understood and appreciated from the following detailed description taken in conjunction with the drawings in which:

Fig. 1 is a schematic illustration of a signature authentication system according to one embodiment of the present invention;

Fig. 2 is a schematic illustration of a signature authentication system according to one embodiment of the present invention;

Fig. 3 is a flow chart of a method of providing a reference signature according to the invention;

Fig. 4 is a flow chart of a method of authenticating a signature;

Fig. 5 is a detail of a method of comparing the signature in the method of Fig. 4; and

Fig. 6 is a flow chart of a method of updating a reference signature.

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to a system and method for authenticating signatures, the system and method being suitable also for authenticating signatures transmitted over communication lines. The present invention uses signature vector recognition and is based on the use of a digitizer together with software in a dynamic identification unit which calculates parameters based on data produced during signature by the electronic pen on the digitizer tablet. These

parameters, which are unique to each person when he signs his own name, are compared with the parameters in a reference signature record, or personal signature profile, which is based on data produced during a number of signatures, to determine whether the signature is authentic (i.e., signature by the authorized signatory) or forged.

For purposes of the present invention, a digitizer refers to any device which converts a location on an X,Y tablet, possibly with the angle of the pen and the pressure on the pen, to a numerical value, and an electronic pen is any device by which a person can write or sign on a digitizer tablet such that parameters of his handwriting can be detected by the digitizer. It will be appreciated that the system can be used to authenticate the handwriting of any predetermined word or words for which a reference record is made. Since the most common words used to identify a person are his signature, the present application refers to signatures, by way of non-limiting example, only.

It will be appreciated that there are many instances when it is desirable to authenticate the signature of a signatory, both in legal and business matters. The invention will be described hereinbelow with relation to credit cards, for which it is particularly suitable, by way of example only, but those skilled in the art will appreciate that it can also be applied in any other instance of signature verification where the system components can be made available.

When transmitting the signature over transmission lines for acceptance, as by a bank or credit card company, additional security can be provided by encrypting the signature with a secret key, known only to the signatory and the bank, which cannot be determined by downloading the data containing the signature signals from the transmission line.

Referring now to Fig. 1, there is shown a schematic illustration of a system for authenticating a signature

constructed and operative in accordance with one embodiment of the invention. The system includes a digitizer 10 with an associated electronic pen 12 coupled to a computer 14 for authenticating a signature at the time and place of signature. This system is particularly suitable for point of sale use. Digitizer 10 can be any conventional digitizer, such as a Wacom Digitizer, manufactured by Wacom Co. Ltd., Japan.

The signatory carries an Integrated Chip (IC) card, or smart card 15 on which is stored a reference signature record, or personal signature profile, for the signatory. Computer 14 includes a comparator 17, which compares the signature to be authenticated with the reference signature record stored on IC card 15. If the signature is within predefined tolerances of the reference signature, comparator 17 sends an accept signal to computer 14. If the signature is not within the predefined tolerances of the reference signature, comparator 17 sends a reject signal to computer 14.

Referring now to Fig. 2, there is shown a schematic illustration of a system for authenticating a signature constructed and operative in accordance with an alternative embodiment of the invention. The system includes a digitizer 10' with an associated electronic pen 12' coupled to a computer 14' having a modem (not shown) for transmitting data from computer 14' to a remote location 16, generally a bank or credit card company in the present example.

At remote location 16, the data is received by a dynamic identification unit 20 arranged to receive the data produced during signature by the electronic pen on the digitizer tablet and calculate therefrom a table of parameters which constitutes a signature record. The result is provided to a comparator 22 which compares the signature to be authenticated with a reference signature record, or personal signature profile, stored in its memory 24. If the signature

is within predefined tolerances of the reference signature, comparator 22 sends an accept signal to computer 14'. If the signature is not within the predefined tolerances of the reference signature, comparator 22 sends a reject signal to computer 14'.

Operation of the system of the invention is as follows. First, a reference signature record, or personal signature profile, must be provided for the bank or credit card company or other body which must accept or reject the signature, as shown in Fig. 2. This is done at the time of opening an account or requesting a credit card. The user signs his name on a digitizer tablet coupled to the computer of the credit card company. The pen position over the tablet is recorded by the computer to produce vectors, and a mathematical analysis is performed to learn the following parameters at any given time during the signature process:

pen position (X,Y coordinates) over the tablet;

sequences of drawing: number of letters, relative position, and time to draw;

acceleration and deceleration during signature;

direction changes.

Optionally the computer can also calculate pen tilt relative to the tablet and pen pressure, if the digitizer used is capable of providing this data. The digitizer data of the signature are input 30 to the dynamic identification unit in the computer. The dynamic identification unit records 32 the parameters of the signature. The recorded parameters are arranged 34 in a table of parameters. This process is repeated 36 a predetermined number of times, for example between 5 and 10, so as to permit the dynamic identification unit to calculate the tolerances 38 associated with the variations in the individual's signature, which is never identical. It will be appreciated that the range of acceptable variations in a personal signature profile will vary from person to person. Once the parameter table and

tolerances have been determined, these are stored in the computer memory for later reference as the reference signature record. It will be appreciated that, preferably, the personal signature profile consists of an array of parameters and logical tolerances or permitted variations, not an "average" signature.

A personal ID code is also recorded 39 together with the signature vector table. This personal ID code serves as an encryption key to provide additional security for signature data transmitted over transmission lines. This encryption key can be any string selected by the user which is known only to him and the credit card company. While the password selected by the credit card company, which is used in cash machines, etc. in conventional credit card authentication systems, can be used as the encryption key, it is preferable to select a key which does not appear on the card. One example of a suitable encryption key is the user's birthdate.

It is a particular feature of the invention that the dynamic identification unit will recognize a person's signature even if it is signed upside down (i.e., where the cardholder is in front of a counter) or rotated to any other angle, where the signature is smaller or larger in size, or slightly different in details.

At the time of making a credit card purchase, the purchaser's signature is authenticated as follows, as shown in Fig. 3. The customer signs with an electronic pen on a digitizer tablet in the store or on the digitizer tablet coupled to his home computer. The record of the signature is received 40 by the credit card company. The dynamic identification unit retrieves 42 the reference signature record of the cardholder. It may also retrieve 44 the personal ID code of the cardholder from the company computer if the signature is encrypted with the personal ID code. Generally this is necessary when making purchases other that at point of sale. If the record of the signature was

encrypted (described in detail hereinbelow) the record is now decrypted 46. If no recognizable signature record is received 48, the signature is rejected.

If the decryption results in a recognizable signature record, or if the signature record was not encrypted, the dynamic identification unit proceeds to identify the signature 50, as shown in detail in Fig. 4. The dynamic identification unit traces 52 the vector lines in the signature record and fills a parameter table 54 with the various parameters. The parameter table of the signature record is compared 56 with the reference parameter table stored in the computer memory.

Parameters for comparison are selected, for example, from the characteristics listed above. Any or all may be selected for use by the programmer. For example, the comparator can determine whether there is a significant difference in time of writing the signature 58, which could indicate copying rather than an authentic signature. It can determine whether there is a difference in the number of vectors 60, i.e., whether a letter has been added or omitted. It can look for a change in the angle of the pen 62. It can determine whether there is a change in the relative direction of the signature 63. And it can determine whether there are differences in pressure during signing 64. If any of the examined parameters is significantly different, i.e., outside the range of tolerances 66 (Fig. 3), the signature will be rejected. If the signature record meets all the characteristics of the reference signature record, the signature will be authenticated and accepted. An indication of acceptance is then sent to the point of purchase.

When making transactions at the point of sale, generally the physical lines are sufficiently secure that no encryption is required, although it can be used, if desired. However, for transactions over the Internet, encryption is recommended to prevent theft of the credit card details. In this case,

the Web surfer will have his own digitizer tablet coupled to his computer. After typing in the credit card number, as in conventional credit card purchases over the net, a signature authentication software driver will pop an input window to the cardholder's screen. The cardholder will type his personal ID code and then sign his name on the digitizer tablet. The vectors produced during signature on the digitizer tablet are calculated and the software encrypts the signature data using the personal ID code as the encryption key, as known.

The encrypted signature record is sent to the vendor, which may be a site on the Internet. The vendor forwards the signature record, as is, to the credit card company for authentication of the signature. When the encrypted signature record reaches the credit card company, it is authenticated as described above with reference to Figs. 3 and 4. When the reference signature data of the cardholder is retrieved, the encryption key is also retrieved, permitting the dynamic identification unit to decrypt the signature record and compare it with the reference signature. In accordance with the results of the comparison, the credit card company will notify the vendor that the signature is accepted or rejected.

Preferably, the authenticating computer will include means for detecting hacking. For example, if two identical signatures are received, one after another, the computer is preferably programmed to reject the second signature, even if it falls within the personal signature profile. This is because, in real life, no one signs his or her name exactly the same way twice in a row.

On the other hand, over time, a person's signature tends to change. Therefore, according to a preferred embodiment of the invention, updating means is provided for changing the personal signature profile or reference signature record, in accordance with perceived, consistent changes in the

signature. A flow chart of one example of suitable software for accomplishing this updating is illustrated in Fig. 5.

In Fig. 5, the comparator receives the signature for authentication and compares it with the personal signature profile (block 70). If the result is not close to the edge of the tolerances or permitted variations, the comparator exits the program (block 72). If the result is close to the edge of the tolerances or permitted variations, an invalid counter is incremented by one (block 74). The counter is checked (block 76) and, if the result is less than a pre-selected number, e.g. 5, the comparator exits the program (block 78). If the results equals the pre-selected number, the old signature is replaced by the new signature (block 80), and the Tolerance Table is rebuilt to include the new signature parameters and permitted variations (block 82). At the same time, the Invalid Counter is cleared.

According to another embodiment of the invention, the signature authentication is utilized for network access, instead of a password. In this embodiment, the personal signature profile is provided to the network, in lieu of a personal passwork. When access to the network is desired, the user signs a digitizer coupled to his workstation, and the signature is compared with the personal signature profile. This method greatly increases security within the network, by preventing access to a hacker who discovered the password by unauthorized means, or to an unauthorized person who was given the password.

It will be appreciated that the invention is not limited to what has been described hereinabove merely by way of example. Rather, the inventon is limited solely by the claims which follow.

CLAIMS

1. A system for authenticating a signature comprising:

(a) a digitizer and associated electronic pen ;

(b) a dynamic identification unit for receiving data from said digitizer produced during signature by said electronic pen on said digitizer, calculating signature parameters and permitted variations from said data, and generating a reference signature record therefrom;

(c) a comparator for comparing said received parameters produced during signature with said reference signature record; and

(d) apparatus for providing an accept or reject response in accordance with the output of said comparator.

2. The system according to claim 1, further comprising:

a transmitter for transmitting said calculated signature parameters for authentication; and

a receiver for receiving said transmitted signature parameters, said receiver being coupled to said comparator.

3. The system according to claim 2, wherein:

(a) said system further includes an encryptor for encrypting said measured parameters to provide an encrypted signature record; and

(b) said dynamic identification unit further includes a decoder for decoding said encrypted signature record.

4. The system according to claim 1, wherein said reference signature record is stored on an IC (integrated chip) card.

5. The system according to any of claims 1 to 3 for authenticating a signature transmitted over a transmission line comprising:

(a) a vendor unit including:

(1) a digitizer and associated electronic pen; and

(b) a signature authorization unit coupled to said vendor unit by the transmission line and including:

(1) a dynamic identification unit for receiving data from said digitizer produced during signature by said electronic pen on said digitizer, calculating signature parameters therefrom, and generating a reference signature record corresponding thereto;

(2) a comparator for comparing said parameters produced during signature with said reference signature record; and

(3) apparatus for providing an accept or reject response to said vendor unit in accordance with the output of said comparator.

6. The system according to claim 2 or 3 for authenticating a signature transmitted over communication transmission lines comprising:

(a) a cardholder unit including:

(1) a digitizer and associated an electronic pen;

(2) apparatus for transmitting the output of said digitizer over the communication transmission lines;

(b) a signature authorization unit including:

(1) a dynamic identification unit for receiving data from said digitizer produced during signature by said electronic pen on said digitizer, calculating signature parameters therefrom, and generating a reference signature record corresponding thereto;

(2) a comparator for comparing said parameters produced during signature with said reference signature record; and

(3) apparatus for providing an accept or reject response in accordance with the output of said comparator; and

(c) a vendor unit coupled to said cardholder unit and to said signature authorization unit by the communication transmission lines and including a transceiver for receiving said output of said digitizer from said cardholder unit and transmitting it to said signature authorization unit; and for receiving said accept or reject response from said signature authorization unit.

7. The system according to any of the preceding claims, wherein said reference signature record includes an array of signature parameters and permitted variations.

8. The system according to any of the preceding claims, further comprising means for updating said reference signature record.

9. A method of authenticating a signature including the steps of:

(a) providing a reference signature record;

(b) signing with an electronic pen on a digitizer tablet;

(c) calculating signature parameters from data received from said digitizer produced during signature by said electronic pen on said digitizer;

(d) comparing said parameters produced during signature with said reference signature record; and

(e) providing an accept or reject response in accordance with results of the comparison.

10. The method according to claim 9, and further including the steps of:

(a) encrypting said calculated parameters with a encryption key after said step of calculating; and

(b) decrypting said encrypted parameters before comparing said parameters.

11. The method according to claim 9, wherein said step of providing a reference signature record includes:

(a) writing the signature on said digitizer several times;

(b) calculating signature parameters for each signature;

(c) calculating permitted variations of said signature parameters; and

(d) storing said signature parameters and said permitted variations as a reference signature record.

12. The method according to any of claims 9 to 11, further comprising updating said reference signature record.

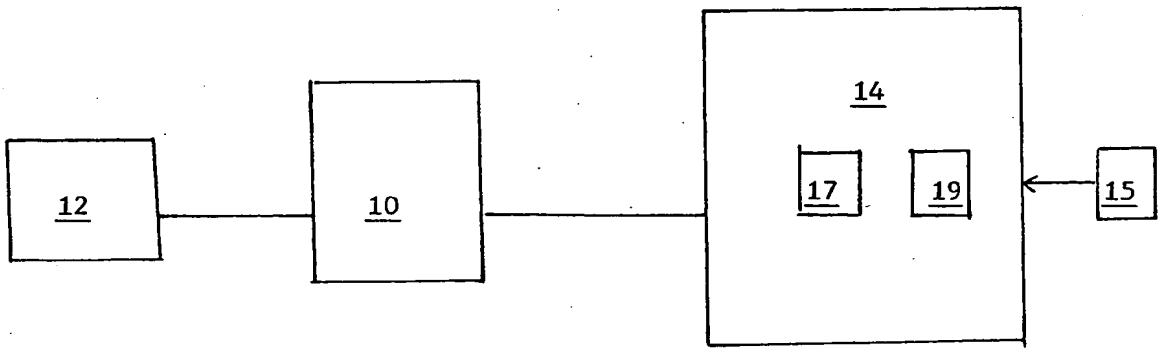


FIG. 1

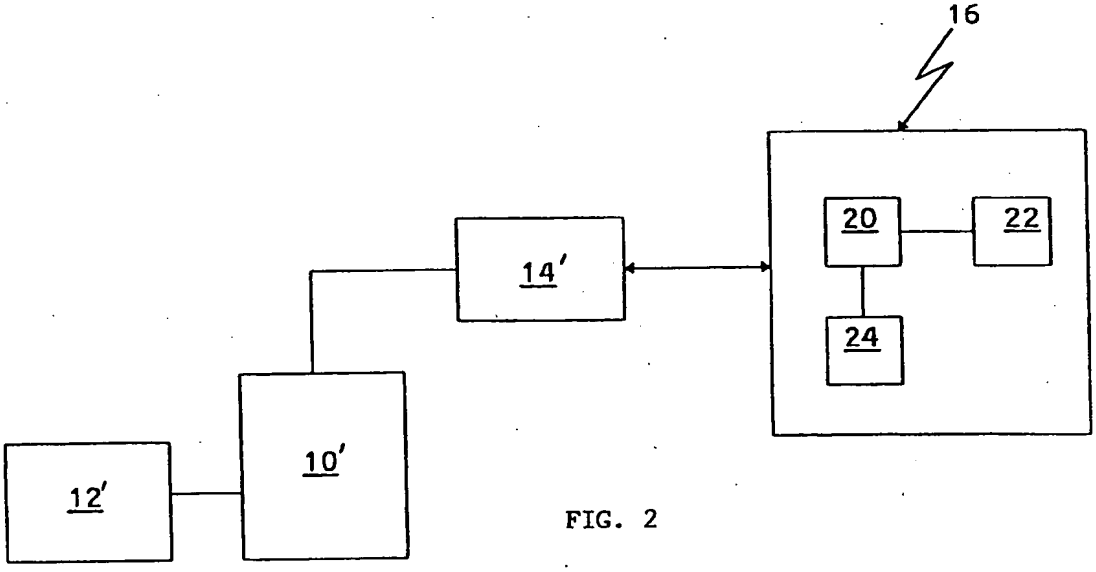


FIG. 2

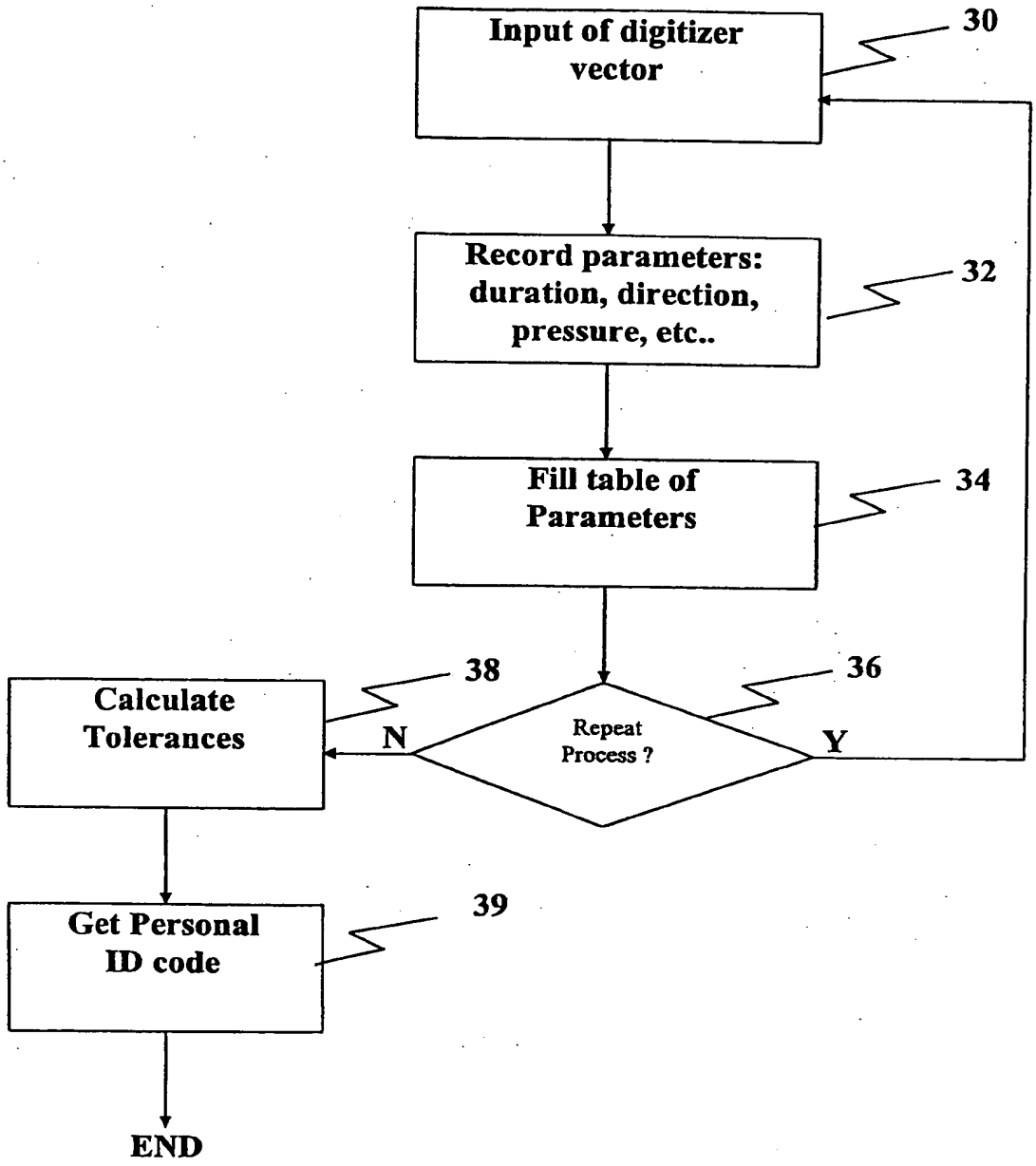

Input of digitizer vector
30
Record parameters: duration, direction, pressure, etc..
32
Fill table of Parameters
34
Repeat Process ?
36
N
Y
Calculate Tolerances
38
Get Personal ID code
39
END

Fig. 3

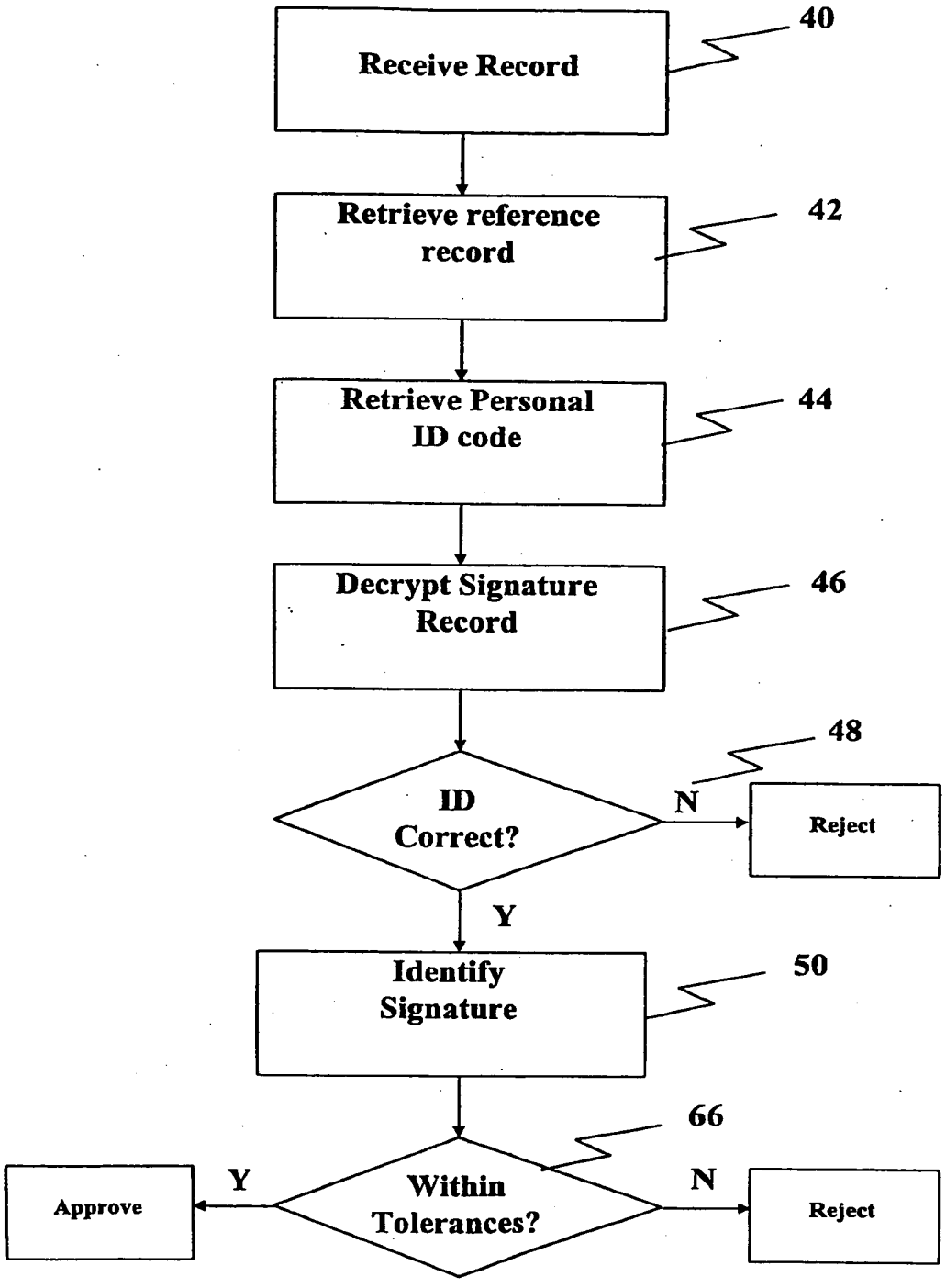

Receive Record
40
Retrieve reference record
42
Retrieve Personal ID code
44
Decrypt Signature Record
46
ID Correct?
48
N
Reject
Y
Identify Signature
50
66
Approve
Y
Within Tolerances?
N
Reject

Fig. 4

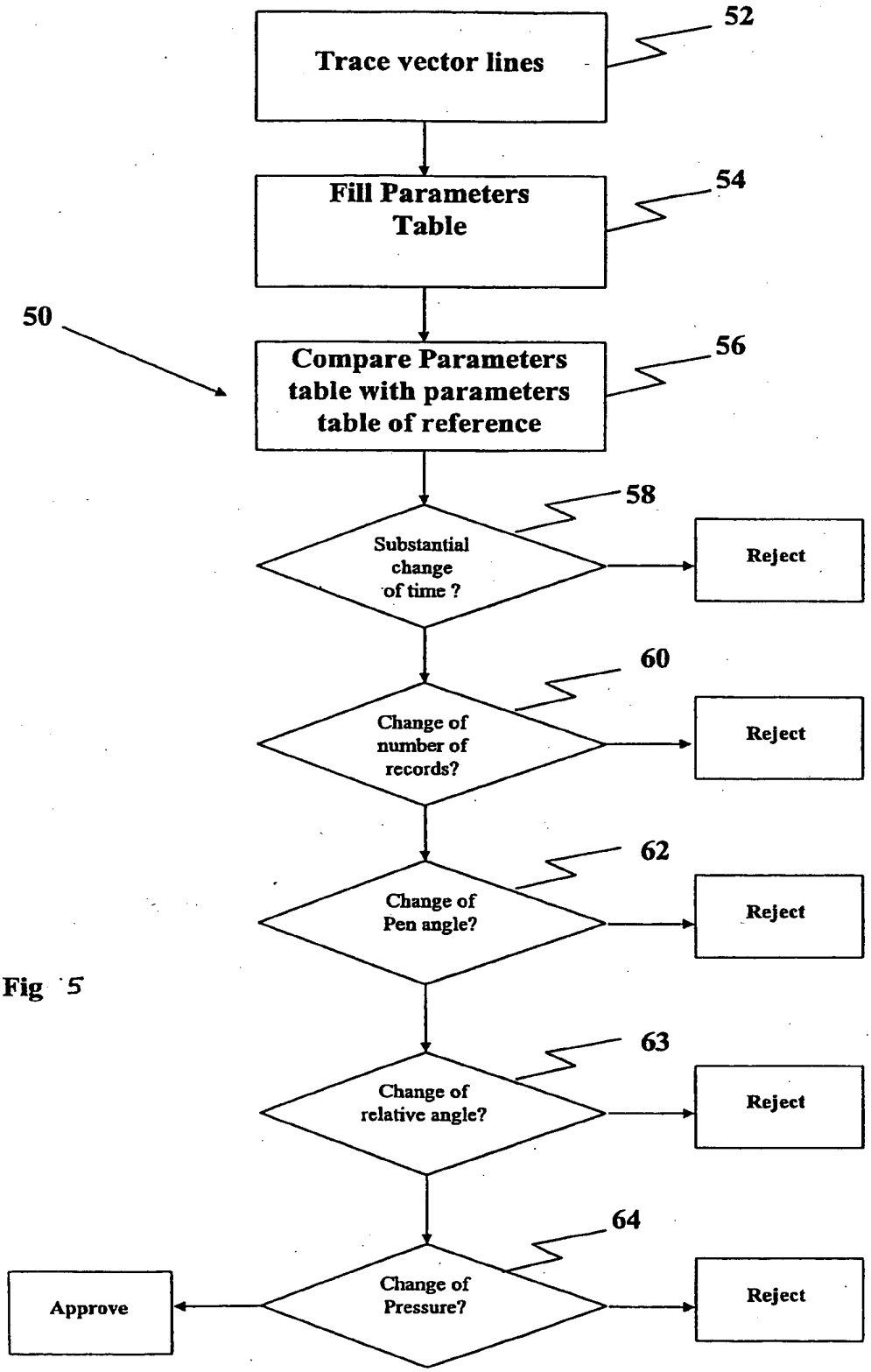

Trace vector lines
52
Fill Parameters Table
54
50
Compare Parameters table with parameters table of reference
56
58
Substantial change of time ?
Reject
60
Change of number of records?
Reject
62
Change of Pen angle?
Reject
63
Change of relative angle?
Reject
64
Change of Pressure?
Reject
Approve

Fig 5

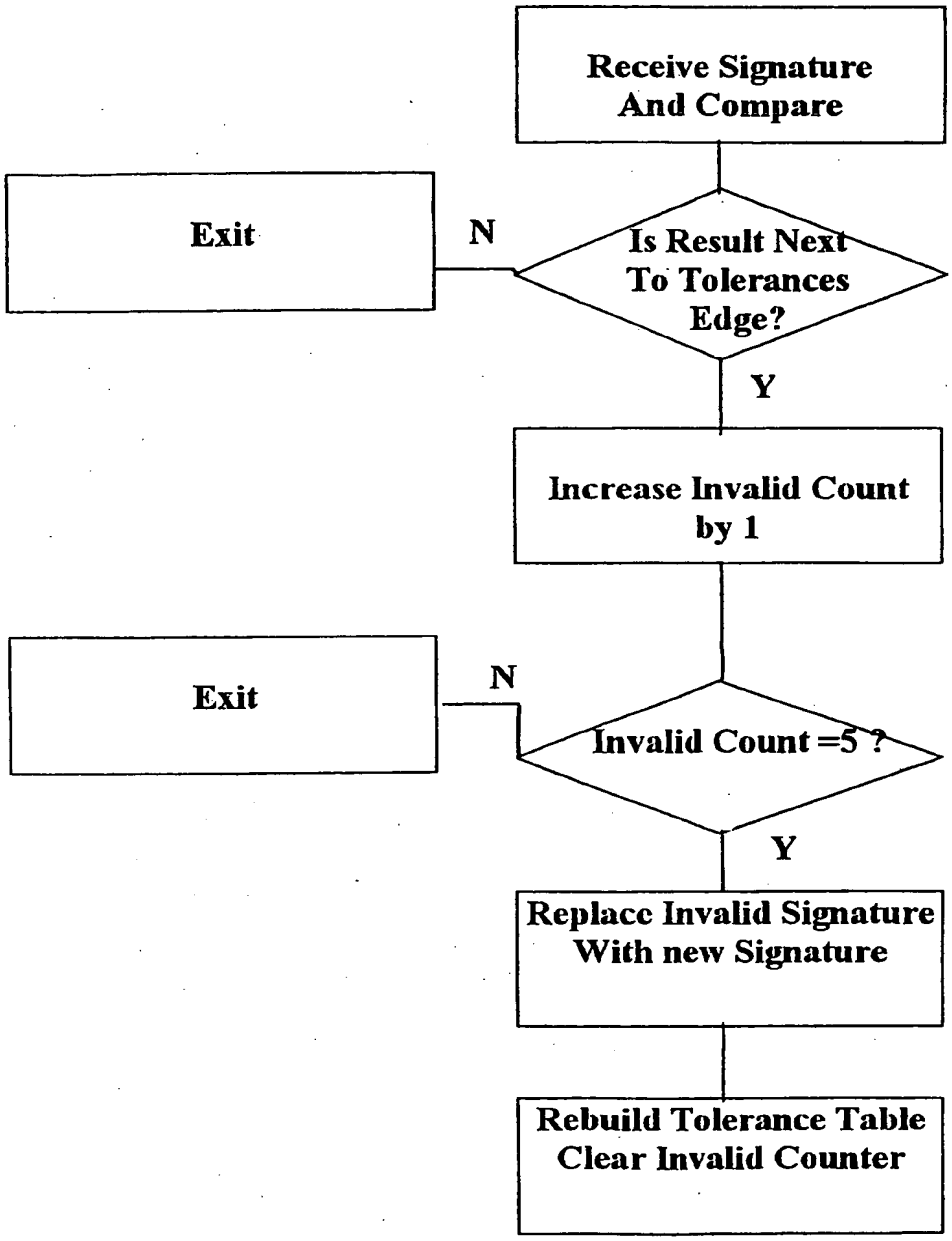

Receive Signature And Compare
Is Result Next To Tolerances Edge?
N
Exit
Y
Increase Invalid Count by 1
Invalid Count =5 ?
N
Exit
Y
Replace Invalid Signature With new Signature
Rebuild Tolerance Table Clear Invalid Counter

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00342

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/23

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23, 3,25; 382/119

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,150,420 A (HARAGUCHI) 22 September 1992, see entire document, especially Fig. 4.	1-12
Y	US 5,195,133 A (KAPP et al) 16 March 1993, See Fig. 5.	1-12
A	US 5,222,138 A (BALABON et al) 22 June 1993, See Fig. 2.	1-12
Y	US 5,297,202 A (KAPP et al) 22 March 1994, See Fig. 5.	1-12
Y	US 5,434,928 A (WAGNER et al) 18 July 1995, See Figs. 1-10	1-12
Y	US 5,544,255 A (SMITHIES) 06 August 1996, See Fig. 4.	1-12

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"B"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 09 OCTOBER 1998	Date of mailing of the international search report 03 NOV 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer SALVATORE CANGIALOSI Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00342

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 5,699,445 A (WAGNER et al) 16 December 1997, See Fig.1.	1-12